

JP:KN

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

-against-

MICHAEL CONLON,

AND

PREMISES KNOWN AND DESCRIBED AS
1490 HORNELL LOOP, APT. 13F
BROOKLYN, NY 11239,

Defendant.

- - - - - X

ROSANNA LICITRA, being duly sworn, deposes and says
that she is a Senior Special Agent with the Department of
Homeland Security, Immigration and Customs Enforcement Agency
("ICE"), duly appointed according to law and acting as such.

Upon information and belief, in or about and between
June 2006 and July 2006, both dates being approximate and
inclusive, within the Eastern District of New York and elsewhere,
the defendant MICHAEL CONLON did knowingly transport and ship in
interstate commerce by computer, child pornography, in violation
of Title 18 United States Code section 2252A.

Upon information and belief, there is probable cause to
believe that there is kept and concealed within the PREMISES
KNOWN AND DESCRIBED as 1490 HORNELL LOOP - APT. 13F

M-06-1181

SEALED

AFFIDAVIT IN
SUPPORT OF
APPLICATION FOR A
SEARCH and ARREST WARRANT

(18 U.S.C. §§ 2252A)

BROOKLYN, NY 11239 (the "Subject Premises") computerized information and material that constitutes evidence or instrumentalities of the possession, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252A.

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Senior Special Agent with ICE and have been so employed for approximately nine years. I am currently assigned to the Child Exploitation Unit, New York City, New York. As an ICE Senior Special Agent, I am currently assigned to investigations relating to, among other things, crimes against children, including the trafficking of child pornography. As part of my responsibilities, I have been involved in the investigation of dozens of child pornography cases. I have been involved in numerous investigations in which child pornography was stored, viewed, and/or transmitted by computer. During the course of these investigations, I have reviewed hundreds of photographs involving child pornography, specifically, photographs which depict minor children (less than 18 years of age) involved in sexual activity. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. This affidavit is in support of an application to search the SUBJECT PREMISES and in support of an arrest warrant for defendant MICHAEL CONLON. For the reasons set forth below, your deponent submits that there is probable cause to believe that computerized and other information is contained within the SUBJECT PREMISES that is evidence and/or instrumentalities of offenses relating to possession, transportation and receipt of child pornography, in violation of Title 18, United States Code, Sections 2252A.

3. The items to be seized are computers, computer hardware, software, related documentation, passwords, data security devices, any video cassette tapes or digital video discs ("DVD"), photographs and data contained therein. These items are further defined in Exhibit A, attached hereto.

4. The factual information supplied in this application and affidavit is based upon my investigation and upon information provided to me orally and in written form by agents of ICE and other law enforcement officers. Because this Affidavit is being submitted for the limited purpose of securing an arrest warrant and a search warrant, I have not set forth every fact resulting from the investigation. Additionally, statements attributed to individuals in this affidavit are described only in sum and substance and in part.

SUBJECT PREMISES

5. The SUBJECT PREMISES located at 1490 HORNEILL LOOP, BROOKLYN, NY, is a seventeen-story brown brick apartment complex. On the awning over the front door is the number "1490." The United States Postal Service confirms that MICHAEL CONLON is presently receiving mail at 1490 HORNEILL LOOP, APT. 13F, BROOKLYN, NY 11239. In addition, MICHAEL CONLON is the only individual receiving mail at the SUBJECT PREMISES. A check of records maintained by the New York State Department of Motor Vehicles revealed that there is a motorcycle registered to MICHAEL CONLON, 1490 HORNEILL LOOP, APT. 13F, BROOKLYN, NY. The motorcycle is the only vehicle registered to the SUBJECT PREMISES. There is no evidence that anyone lives with MICHAEL CONLON at the SUBJECT PREMISES.

THE INTERNET

6. The internet is a global network which allows for the sharing of data across through computers attached to the network.

7. The internet uses a portion of the existing public telecommunication networks. Technically, what distinguishes the internet from traditional circuit based communications is its use of a set of protocols called Transmission Control Protocol (TCP) and Internet Protocol (IP). Protocol is a set of rules that allows for seamless communications between disparate networks.

8. Individual users typically access the internet through a local Internet Service Provider (e.g., America Online, CompuServe, Optimum On-line) through a modem or other connection device, such as a cable or Digital Subscriber Line (hereinafter referred to as "DSL").

9. Individuals can use online resources to retrieve and store child pornography, including services offered by Internet Portals such as America Online (AOL), Yahoo!, Google, and Hotmail, among others. Online services allow a user to set up an account providing e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

Google "Hello" Program

10. Google's "Hello" software program is a new Internet service that enables users to trade images easily, quickly, and securely. The Hello program lets traders connect directly (peer-to-peer) to each other's computers specifically for the purpose of sharing pictures. Since the connection is peer-to-peer, there is no limit to the number and size of pictures that may be shared.

11. The user is asked to create the following information: User name or "handle", email address, and password. The user is then given access to download the installation file. Google sends a verification email to the email address provided during the registration. Each account will also have a unique User Identification number (UID) assigned by the Hello software.

BACKGROUND OF THE INVESTIGATION

12. In March of 2005, the United States Immigration Customs Enforcement (ICE), Special Agent in Charge Seattle, Washington (SAC/Seattle) office began to investigate Internet users involved in the distribution and receipt of child pornography via the Google "Hello" File Sharing program. One of these users was later identified as Washington State resident Nicholas Farmer. Information gathered during the Farmer investigation revealed that Farmer had used the Hello screen name "Farmer420" to distribute and receive images of child pornography. Based on this information, SAC/Seattle agents obtained a federal search warrant for Farmer's residence.

13. On July 13, 2006, SAC/Seattle agents and members of the Seattle Internet Crimes Against Children (ICAC) Task Force served the search warrant. The search warrant resulted in the seizure of evidence pertaining to the distribution and receipt of child pornography.

14. On or about July 17, 2006, a SAC/Seattle Computer Forensic Agent (CFA) extracted the Google Hello files located on Farmer's computer.

15. Of particular interest were the Google Hello files containing images received from Hello UID number 1103936. The files recovered from Farmer's computer listed the UID number 1103936 handle as "phamilyguy" with an email address of "phamily_guy@yahoo.com.

16. Phamilyguy subsequently sent at least 12 images to Farmer between June 2006 and July 2006. All of those images depicted child pornography (i.e., prepubescent girls and boys performing oral sex and having sexual intercourse with adult males). I have reviewed those images and based on my training and expertise believe them all to contain depictions of child pornography. Moreover, based on my discussions with other ICE agents, I know that at least one of children contained in the images sent by Phamilyguy has been identified as a seven year old female residing in Washington State.

17. Pursuant to a subpoena, Google Inc. has verified that the Google Hello user identification number 1103936 is registered to user name Phamilyguy with e-mail address of phamily_guy@yahoo.com.

18. Pursuant to a subpoena, Yahoo! Inc. has verified that the e-mail address phamily_guy@yahoo.com is registered to

george bush, Brooklyn, NY. Yahoo! also provided IP address used by phamily_guy@yahoo.com which identifies the location of the computer used by phamily_guy@yahoo.com to send the subject images. That address is 1490 HORNELL LOOP, APT. 13F, BROOKLYN, NY 11239, the SUBJECT PREMISES.

19. Pursuant to a subpoena, Cablevision Systems Corp. has verified that MICHAEL CONLON, 1490 HORNELL LOOP, APT. 13F, BROOKLYN, NY 11239 has an active account with their company.

20. Based on the factual information provided herein, your deponent believes that defendant MICHAEL CONLON maintains computers and associated peripheral equipment at the SUBJECT PREMISES and that such computers and equipment were used to transmit child pornography over the internet and in interstate commerce.

21. Based upon the facts set forth herein and the training and experience of your deponent, there is probable cause to believe that the items listed on Exhibit A attached herewith, which is incorporated by reference herein, will be found at the SUBJECT PREMISES and that those items constitute evidence, fruits and instrumentalities in violation of the federal child pornography law, 18 U.S.C. Sections 2250 and 2252A.

22. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to

examine, analyze, and test them. Based upon my knowledge, training and experience, and consultations with FBI experts, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

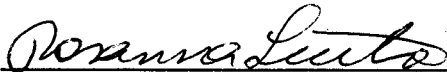
(a) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data store, and it would be impractical to attempt this kind of data search on site.

(b) Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which

expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive codes imbedded in the system as a "booby trap") a controlled environment is essential to its complete and accurate analysis.

23. Based on the factual information contained herein, probable cause exists to conclude that the SUBJECT PREMISES will contain evidence of violations of 18 U.S.C. Sections 2252A and that probable cause exists to believe that MICHAEL CONLON did knowingly send child pornography, in violation of 18 U.S.C. Sections 2252A.

WHEREFORE, your deponent respectfully requests that the Court (A) issue a search warrant for the items listed in Exhibit A of this affidavit, all of which constitute fruits, instrumentalities and evidence of the violation of 18 U.S.C. Section 2252A and (B) issue an arrest warrant for the defendant MICHAEL CONLON so that he may be dealt with according to law.



Rosanna Licitra
Senior Special Agent, ICE
New York Division

Sworn to before me this
13th day of November, 2006

JMA

UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

Exhibit A

ITEMS TO BE SEIZED

1. A computer, computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, video recording devices, video recording players, monitors and or televisions, and data were instrumentalities of and will contain evidence related to this crime. The following definitions apply to the terms as set out below:

(A) Computer Hardware

Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (such as central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (such as keyboards, printer, attached video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks.)

(B) Computer Software

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications and utilities.

(C) Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

(D) Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may

include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

2. Any and all records, documents, invoices and materials that concern any accounts with America On-Line or any other internet service provider.

Any of the items described in paragraphs 1 through 2 above which are stored by MICHAEL CONLON in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices, whether performed on site or in a laboratory, or other controlled environment, may include the following techniques:

(a) surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

(b) "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

(c) "scanning" storage areas to discover and possibly recover recently deleted data;

(d) "scanning" storage areas for deliberately hidden files;
or

(e) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

This warrant and this search procedure specifically excludes a search of any kind of unopened electronic mail. No search of unopened electronic mail shall be conducted without a separate search warrant supported by probable cause. Appropriate efforts shall be made to minimize the disclosure of records and other information which are not the subject of this warrant.